

# A bound for the size of the sum of dilates

George Shakan

University of Wyoming Department of Mathematics  
Laramie, Wyoming 82072, USA  
gshakan@uwyo.edu

February 25, 2014

## Abstract

We show for any  $\lambda_1, \dots, \lambda_k \in \mathbb{Z}$ , satisfying the condition that for every  $2 \leq j \leq k$  there is an  $i < j$  such that  $(\lambda_i, \lambda_j) = 1$ , and any finite  $A \subset \mathbb{Z}$  one has

$$|\lambda_1 \cdot A + \dots + \lambda_k \cdot A| \geq (|\lambda_1| + \dots + |\lambda_k|)|A| - C,$$

where  $C$  only depends on  $\lambda_1, \dots, \lambda_k$ . We also show if  $B$  is a finite subset of the integers such that  $\emptyset \neq A \subset B$ , then there is a constant  $C_{\lambda_2}$  depending only on  $\lambda_2$  such that

$$|\lambda_1 \cdot B + \lambda_2 \cdot A| \geq |B| + |\lambda_2||A| - C_{\lambda_2}.$$

## 1 Introduction

Let  $A$  and  $B$  be finite sets of real numbers. The sumset of  $A$  and  $B$  is defined by

$$A + B = \{a + b : a \in A, b \in B\}.$$

For  $d > 0$  the dilation of  $A$  by  $d$  is defined by

$$d \cdot A = \{d\} \cdot A = \{da : a \in A\},$$

while for any real number  $x$ , the translation of  $A$  by  $x$  is defined by

$$x + A = \{x\} + A = \{x + a : a \in A\}.$$

Set  $\lambda_1, \dots, \lambda_k$  to be integers such that for every  $2 \leq j \leq k$  there is an  $i < j$  such that  $(\lambda_i, \lambda_j) = 1$ . Let  $A$  be a finite subset of the integers. Here we are concerned with lower bounds of

$$|\lambda_1 \cdot A + \dots + \lambda_k \cdot A|.$$

Taking  $X = \{0, \dots, |X| - 1\}$ , it follows that

$$\lambda_1 \cdot X + \dots + \lambda_k \cdot X \subset \{0 \dots, (|\lambda_1| + \dots + |\lambda_k|)(|X| - 1)\} + (|X| - 1) \sum_{\{i: \lambda_i < 0\}} \lambda_i,$$

and so

$$|\lambda_1 \cdot X + \dots + \lambda_k \cdot X| \leq (|\lambda_1| + \dots + |\lambda_k|)|X| - (|\lambda_1| + \dots + |\lambda_k| - 1).$$

This shows that a lower bound for  $|\lambda_1 \cdot A + \dots + \lambda_k \cdot A|$  can be at best linear in  $|A|$ . It is reasonable to guess that the multiplicative constant in front of  $|X|$  might be the best possible. Constructions in [1] and [3] show that the additive constant is not optimal. Indeed, in [2] it was shown that

$$|\lambda_1 \cdot A + \dots + \lambda_k \cdot A| \geq (|\lambda_1| + \dots + |\lambda_k|)|A| - o(|A|), \quad (1)$$

with the relaxed condition that  $\lambda_1, \dots, \lambda_k$  simply be coprime. The works of [1, 3, 6, 7] made improvements from  $o(|A|)$  to a constant in certain cases, all when  $k \leq 2$ . The interested reader is directed to the introductions of [1] and [2] for a more complete history of the problem. In this note, we show the following.

**Theorem 1.1.** *Let  $\lambda_1, \dots, \lambda_k$  be integers such that for every  $2 \leq j \leq k$  there is an  $i < j$  with the property that  $(\lambda_i, \lambda_j) = 1$  and  $A$  be a finite subset of the integers. Then*

$$|\lambda_1 \cdot A + \dots + \lambda_k \cdot A| \geq (|\lambda_1| + \dots + |\lambda_k|)|A| - C,$$

where  $C$  only depends on  $\lambda_1, \dots, \lambda_k$ .

Note that one may safely reorder  $\lambda_1, \dots, \lambda_k$  to satisfy the hypothesis of Theorem 1.1 without affecting  $|\lambda_1 \cdot A + \dots + \lambda_k \cdot A|$ . One notable case where the hypothesis of Theorem 1.1 is satisfied is when  $(\lambda_1, \lambda_j) = 1$  for all  $2 \leq j \leq k$ . We suspect the result is true for coprime  $\lambda_1, \dots, \lambda_k$  but we are unable to prove it here. For example we cannot improve upon (1) for the set

$6 \cdot A + 10 \cdot A + 15 \cdot A$ . We will confine ourselves to subsets of the integers. Transforming our result to the case where the set  $A$  is from rationals is an obvious task by clearing denominators. There is Freiman isomorphism (see definition 5.21 in [10]) of arbitrarily large order from any finite set of real numbers to a finite set of integers (see Lemma 5.25 in [10]). Thus Theorem 1.1 extends to  $A$  being a finite subset of the real numbers.

We would like to take a slight detour and discuss the analogous problem for finite fields of a prime order,  $p$ . The problem appears to be harder and much less is known. The only exact result in this direction is the celebrated Cauchy-Davenport theorem. Even the behavior of  $|A + 2 \cdot A|$  when  $A \subset \mathbb{F}_p$  is unclear. Both [8] and [9] have partial results in this direction, but the general question remains open. Constructions in [9] show that when  $A \subset \mathbb{F}_p$  is large with respect to  $p$ ,  $|\lambda_1 \cdot A + \dots + \lambda_k \cdot A|$  can be smaller than what would be expected from the case where  $A \subset \mathbb{Z}$ . In Corollary 2.2 in [9], it is shown that for very small  $A \subset \mathbb{F}_p$ ,

$$|\lambda_1 \cdot A + \dots + \lambda_k \cdot A| \geq (|\lambda_1| + \dots + |\lambda_k|)|A| - o(|A|),$$

by using Theorem 1.2 in [5] to transfer the problem to the integers and then using the result for the integers proved in Theorem 2 of [2]. We remark that the same method works with Theorem 1.1 in place of Theorem 2 in [2] to improve  $o(|A|)$  to a constant, when  $\lambda_1, \dots, \lambda_k$  are integers such that  $(p, \prod_{i=1}^k \lambda_i) = 1$  and for every  $2 \leq j \leq k$  there is an  $i < j$  such that  $(\lambda_i, \lambda_j) = 1$ .

## 2 Preliminaries

Let  $A$  be a finite subset of the integers and  $p, q \in \mathbb{Z}$  such that  $(p, q) = 1$ . In [1], it was shown that

$$|p \cdot A + q \cdot A| \geq |p \cdot A + q \cdot A| \geq (|p| + |q|)|A| - C_{p,q}, \quad (2)$$

where  $C_{p,q}$  is a constant that only depends  $p$  and  $q$ . It was assumed that  $p, q > 0$  in [1], but (2) is true with identical proof. We remark that only the proof of Lemma 2.1 in [1] uses that  $p, q > 0$ , but one may establish this fact using our proof of Lemma 3.2, which does not make this assumption. Here we prove a result of a similar flavor.

**Theorem 2.1.** *Let  $p, q \in \mathbb{Z}$  such that  $(p, q) = 1$ . Let  $A$  and  $B$  be finite, nonempty subsets of the integers such that  $A \subset B$ . Then*

$$|p \cdot B + q \cdot A| \geq |B| + |q||A| - q^2 2^{(|q|-1)^2}.$$

One may easily check in the case where  $0 < |p| < |q|$ ,  $X = \{1, \dots, |X| \geq |q|\}$ , and  $Y = \{x \in X : p \mid x\}$ , one has  $Y \subset X$  and  $|p \cdot X + q \cdot Y| = |X| + |q||Y| - |q|$ . Note that when  $p = 1$ , Theorem 2.1 is strictly a generalization of the case  $p = 1$  in (2) which allows one to replace  $A + q \cdot A$  with  $B + q \cdot A$  for any nonempty  $A \subset B$ .

We now show how to use Theorem 2.1 to improve  $o(|A|)$  in (1) to a constant in the case where  $\lambda_1, \dots, \lambda_k$  are integers having the property that for every  $2 \leq j \leq k$  there is an  $i < j$  such that  $(\lambda_i, \lambda_j) = 1$ . We prove by induction, needing Theorem 1.1 in [1] to start the induction.

*Proof of Theorem 1.1.* We prove by induction on  $k$ ,  $k = 1$  being obvious and  $k = 2$  being proved in Theorem 1.1 in [1]. Assume  $k \geq 3$ . Translation does not affect  $|\lambda_1 \cdot A + \dots + \lambda_k \cdot A|$ , so we may suppose  $0 \in A$ . Set

$$B := \lambda_1 \cdot A + \dots + \lambda_{k-1} \cdot A.$$

By our assumption, we may assume  $(\lambda_i, \lambda_k) = 1$  for some  $1 \leq i \leq k-1$ . Since  $0 \in A$ ,

$$\lambda_i \cdot A \subset B.$$

It follows by Theorem 2.1, since  $(\lambda_i, \lambda_k) = 1$ , that

$$|\lambda_1 \cdot A + \dots + \lambda_k \cdot A| = |B + \lambda_k \cdot A| = |\lambda_i \cdot B + \lambda_k \cdot (\lambda_i \cdot A)| \geq |B| + |\lambda_k||A| - C_{\lambda_k}.$$

We assumed  $k \geq 3$ , so the result follows by induction.  $\square$

We briefly remark here on the additive constant  $C$ . Tracing through the proof of  $k = 2$  in [1] and Theorem 2.1, one may take

$$C = 1 + \sum_{i=3}^k \lambda_i^2 2^{(|\lambda_i|-1)^2},$$

if  $|\lambda_1| = |\lambda_2| = 1$  and in all other cases take

$$C = (|\lambda_1 \lambda_2|)^{(|\lambda_1|+|\lambda_2|-3)(|\lambda_1|+|\lambda_2|)+1} + \sum_{i=3}^k \lambda_i^2 2^{(|\lambda_i|-1)^2}.$$

We also remark that an inductive proof for the case where  $\lambda_1, \dots, \lambda_k$  are coprime similar to the proof of Theorem 1.1 seems unlikely as Theorem 2.1 is simply not true when  $(p, q) > 1$ . For the rest of the document, we will be concerned with the proof of Theorem 2.1

### 3 Proof of Theorem 2.1

We now turn to preparing the proof of Theorem 2.1. The proof adopts ideas from [1].

Let  $A, B \subset \mathbb{Z}$  be finite and let  $p, q \in \mathbb{Z}$  such that  $(p, q) = 1$ . For convenience, we suppose for the rest of the document that  $q > 0$ . We may assume this since changing  $p, q$  to  $-p, -q$  does not affect  $|p \cdot B + q \cdot A|$ .

We would like to establish some notation. We partition  $B$  into its intersections with residue classes mod  $q$ , that is

$$B = \bigcup_{i=1}^r B_i, \quad B_i = b_i + q \cdot B'_i, \quad B_i \neq \emptyset, \quad 0 \leq b_i < q,$$

where the  $B_j$  are disjoint. It follows that

$$|B| = \sum_{i=1}^r |B_i|$$

and, using  $(p, q) = 1$ , that

$$|p \cdot B + q \cdot A| = \sum_{i=1}^r |p \cdot B_i + q \cdot A|. \quad (3)$$

For nonempty finite subsets of the real numbers  $A = \{a_1 < \dots < a_r\}$  and  $B = \{b_1 < \dots < b_s\}$ , we have that

$$|A + B| \geq |A| + |B| - 1, \quad (4)$$

by observing that

$$a_1 + b_1 < a_2 + b_1 < \dots < a_r + b_1 < a_r + b_2 < \dots < a_r + b_s.$$

This well-known fact establishes Theorem 2.1 when  $q = 1$ , so we may now assume  $q \geq 2$ . We use (4) to modestly generalize Lemma 4 of [3] in the following way.

**Lemma 3.1.** *Let  $A$  and  $B$  be nonempty, finite subsets of the integers and  $p, q \in \mathbb{Z}$  such that  $q \geq 2$  and  $(p, q) = 1$ . Suppose that  $B$  intersects  $r$  residue classes mod  $q$ . Then*

$$|p \cdot B + q \cdot A| \geq |B| + r|A| - r$$

*Proof.* Utilizing (3) and (4), we obtain

$$\begin{aligned} |p \cdot B + q \cdot A| &= \sum_{i=1}^r |p \cdot B_i + q \cdot A| \\ &\geq \sum_{i=1}^r (|B_i| + |A| - 1) \\ &= |B| + r|A| - r, \end{aligned}$$

$$\text{since } |B| = \sum_{i=1}^r |B_i|.$$

□

Now assume  $A \subset B$ . We say  $B$  is fully distributed (FD) mod  $q$  if  $B$  intersects every residue class mod  $q$ , that is  $r = q$ . Note that if  $B$  is FD mod  $q$ , then Theorem 2.1 follows immediately from Lemma 3.1.

Translation and dilation of  $B$  (and  $A$  accordingly) do not affect  $|p \cdot B + q \cdot A|$ . To clarify, we will translate and dilate  $B$ , and it is inferred that the same translations and dilations will be made to  $A$ .

For  $1 \leq i \leq r$ , consider the greatest common divisors

$$d_i = (b_1 - b_i, b_2 - b_i, \dots, b_r - b_i, q).$$

Note that the set  $(B - b_j)/d_j$  still consists of integers. We remark that it is clear that  $(A - b_j)/d_j \subset (B - b_j)/d_j$  also consists of integers. If there is a  $d_j > 1$ , then change  $B$  to  $(B - b_j)/d_j$ . Note that such a change redefines the residue classes  $b_j$  as well as  $r$ .

Repeat this process as many times as possible. If  $|B| \geq 2$  then the process must stop in finitely many steps since each reduction decreases the distance between the minimal and maximal elements of  $B$ .

We say that  $B$  is reduced if the following holds for any  $1 \leq i \leq r$ :

$$(b_1 - b_i, b_2 - b_i, \dots, b_s - b_i, q) = 1. \quad (5)$$

Observe that any reduced set must intersect at least two residue classes mod  $q$  when  $|B| > 1$ . This observation allows us to establish the following. We assume  $B$  is reduced.

**Lemma 3.2.** *Let  $A$  and  $B$  be nonempty, finite subsets of the integers such that  $A \subset B$  and  $p, q \in \mathbb{Z}$  such that  $q \geq 2$  and  $(p, q) = 1$ . Then*

$$|p \cdot B + q \cdot A| \geq |B| + 2|A| - 2$$

*Proof.* If  $|B| = 1$ , the result is obvious. Otherwise, the result follows from the above observation, and the following

$$\begin{aligned} |p \cdot B + q \cdot A| &= |p \cdot B_1 + q \cdot A| + |p \cdot (B \setminus B_1) + q \cdot A| \\ &\geq |B_1| + |A| - 1 + |B| - |B_1| + |A| - 1 = |B| + 2|A| - 2. \end{aligned}$$

□

For  $1 \leq i \leq r$ , let  $A_i = B_i \cap A$  and  $A'_i = \frac{1}{q} \cdot (A_i - b_i)$ . Note that  $A'_i$  is a subset of the integers and it is possible that  $A'_i = \emptyset$ . It is clear that

$$|A| = \sum_{i=1}^r |A_i|.$$

We will need the following lemma.

**Lemma 3.3.** *For any fixed  $1 \leq j \leq r$ , either  $B'_j$  is FD mod  $q$  or*

$$|p \cdot B_j + q \cdot A| \geq |p \cdot B_j + q \cdot A_j| + \min_{1 \leq m \leq r} |A_m|.$$

*Proof.* The result is trivial if for any  $1 \leq i \leq r$ ,  $A_i = \emptyset$ . Suppose

$$|p \cdot B_j + q \cdot A| < |p \cdot B_j + q \cdot A_j| + \min_{1 \leq m \leq s} |A_m|.$$

Then for any  $1 \leq m \leq s$ , we have

$$|A'_m| = |A_m| > |(p \cdot B_j + q \cdot A_m) \setminus (p \cdot B_j + q \cdot A_j)| = |(b_m - b_j + p \cdot B'_j + q \cdot A'_m) \setminus (p \cdot B'_j + q \cdot A'_j)|.$$

It follows that for every  $x \in p \cdot B'_j$  there is a  $y \in A'_m$  such that  $b_m - b_j + x + qy \in p \cdot B'_j + q \cdot A'_j$ , and so there is an  $x' \in p \cdot B'_j$  such that  $b_m - b_j + x \equiv x' \pmod{q}$ . We may repeat this argument with  $x'$  in place of  $x$ , and so on, and we may repeat for all  $m$  so that eventually we get for any  $x \in p \cdot B'_j$  and any  $z = u_1(b_1 - b_j) + \dots + u_s(b_r - b_j)$ , where  $u_1, \dots, u_s$  are arbitrary integers, that there is an  $x' \in p \cdot B'_j$  with  $z + x \equiv x' \pmod{q}$ . Since  $B$  is reduced, the set of  $z$  describes all residues mod  $q$  by (5), and it follows  $p \cdot B'_j$  is FD mod  $q$ . Since  $(p, q) = 1$ , it follows that  $B'_j$  is FD mod  $q$ . □

We remark here that the previous lemma is where the proof fails if one does not assume  $A \subset B$ . Indeed if  $A = \{1, \dots, |A|\}$  and  $B = q \cdot \{1, \dots, |B|\}$ , then  $|B + q \cdot A| = |B| + |A| - 1$ . In this case there is no hope to make  $B$  reduced, without affecting  $|B + q \cdot A|$ .

We are now ready to prove Theorem 2.1. We start with Lemma 3.2 and improve upon it in an iterative way.

**Proposition 3.4.** *Let  $p, q \in \mathbb{Z}$  such that  $q \geq 2$  and  $(p, q) = 1$  and let  $A$  and  $B$  be nonempty, finite subsets of the integers such that  $A \subset B$ . Then for every  $2q \leq m \leq q^2$ ,*

$$|p \cdot B + q \cdot A| \geq |B| + \frac{m}{q}|A| - C_m,$$

where  $C_m$  only depends on  $m$ .

*Proof.* Taking  $m = q^2$  and following the calculation of the additive constant yields Theorem 2.1.

Now we turn to the proof of the proposition. Note that Lemma 3.2 starts the induction with  $C_{2q} = 2$ , but we choose  $C_{2q} = q^2$ . Assume the proposition holds for  $m < q^2$ . We aim to show the proposition holds for  $m'$  where

$$m' = \begin{cases} m + 1 & \text{if } m < q^2 - q \\ \min\{m + 1 - \frac{1}{q}, q^2\} & \text{if } q^2 - q \leq m < q^2 \end{cases}$$

Let  $C_{m'} = 2C_m$ .

Suppose there is a  $1 \leq i \leq r$  such that  $|A_i| \leq \frac{q-1}{m}|A|$ . Clearly  $A \setminus A_i \subset B \setminus B_i$ . Then it follows, using (4) and the induction hypothesis that

$$\begin{aligned} |p \cdot B + q \cdot A| &\geq |p \cdot B_i + q \cdot A| + |p \cdot (B \setminus B_i) + q \cdot (A \setminus A_i)| \\ &\geq |B_i| + |A| - 1 + |B| - |B_i| + \frac{m}{q}(|A| - |A_i|) - C_m \\ &\geq |B| + \frac{m+1}{q}|A| - C_{m'} \geq |B| + \frac{m'}{q}|A| - C_{m'}, \end{aligned}$$

since  $C_{m'} \geq C_m + 1$  and  $m + 1 \geq m'$ . Thus we may assume that  $|A_i| \geq \frac{q-1}{m}|A|$  for all  $1 \leq i \leq r$  and in particular  $A_i \neq \emptyset$ .

Suppose there is a  $1 \leq j \leq r$  such that  $B'_j$  is not FD. Again, we have that  $A \setminus A_j \subset B \setminus B_j$  and also  $A_j \subset B_j$ . Then by Lemma 3.3 and the induction hypothesis we have



$$\begin{aligned}
|p \cdot B + q \cdot A| &\geq |p \cdot B_j + q \cdot A| + |p \cdot (B \setminus B_j) + q \cdot (A \setminus A_j)| \\
&\geq |p \cdot B_j + q \cdot A_j| + \min_{1 \leq m \leq r} |A_m| + |B| - |B_j| + \frac{m}{q}(|A| - |A_j|) \\
&\geq |B_j| + \frac{m}{q}|A_j| - C_m + \frac{q-1}{m}|A| + |B| - |B_j| + \frac{m}{q}(|A| - |A_j|) - C_m \\
&\geq |B| + \frac{m'}{q}|A| - C_{m'},
\end{aligned}$$

since  $C_{m'} \geq 2C_m$ .

Thus we may assume for all  $1 \leq i \leq r$ ,  $B'_i$  is FD and it follows from Lemma 3.1, utilizing that  $A_i \neq \emptyset$ , that

$$|p \cdot B_i + q \cdot A| \geq |p \cdot B'_i + q \cdot A'_i| \geq |B_i| + q|A_i| - q.$$

Taking sums, we see that,

$$\sum_{i=1}^r |p \cdot B_i + q \cdot A_i| \geq \sum_{i=1}^r |B_i| + q|A_i| - q \geq |B| + q|A| - C_{m'},$$

since  $C_{m'} \geq q^2$ .

□

The author would like to thank Antal Balog for not only providing useful suggestions for this paper, but introducing him to the current problem, as well as the beautiful subject of additive combinatorics.

## References

- [1] Balog A and Shakan G. (accepted, to appear) On the sum of dilations of a set. *Acta Arithmetica*
- [2] Bukh B. (2008) Sums of Dilates. *Combinatorics, Probability and Computing* **17** 627–639.
- [3] Cilleruelo J., Hamidoune y. and O. Serra (2009) On sums of dilates. *Combinatorics, Probability and Computing* **18** 871–880.

- [4] Du S. S, Cao H. Q and Sun Z. W. (2014) On a sumset problem for integers. *Electronic Journal of Combinatorics* **21** 1–25.
- [5] Green B. and Ruzsa I. (2006) Sets with small sumset and rectification. *The Bulletin of the London Mathematical Society* **38** 43–52.
- [6] Hamidoune Y. and Rué J. (2011) A lower bound for the size of a Minkowski sum of dilates. *Combinatorics, Probability and Computing* **20** 249–256.
- [7] Ljubic Z. (2013) A lower bound for the size of a sum of dilates. *Journal of Combinatorial Number Theory* **5** 31–51.
- [8] Plagne A. (2011) Sums of dilates in groups of prime order. *Combinatorics, Probability and Computing* **20** 867–873.
- [9] Pontiveros G. (2013) Sum of dilates in  $\mathbb{Z}_p$ . *Combinatorics, Probability and Computing* **22** 282–293.
- [10] Tao T. and Vu V. (2006) *Additive combinatorics*, Cambridge University Press.